IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

KEYPOINT GOVERNMENT SOLUTIONS, INC. **1750 Foxtrail Drive, Suite 120** **Loveland, CO 80538** **Plaintiff,** v. **MICHAEL C. McGINN** **4305 S. Starcrest Dr.** **Warrenton, VA 20187** **Defendant.**	:	**Case No. _____** **JURY DEMAND**

VERIFIED COMPLAINT FOR TEMPORARY RESTRAINING ORDER, PRELIMINARY AND PERMANENT INJUNCTIVE RELIEF, AND OTHER RELIEF

Plaintiff KeyPoint Government Solutions, Inc. ("KeyPoint" and "Plaintiff") complains against Defendant Michael McGinn ("McGinn" and "Defendant") and asserts causes of action for: (1) misappropriation of trade secrets; and (2) conversion, and seeks injunctive relief and other appropriate relief. KeyPoint seeks injunctive relief to stop and further prevent Defendant's use and disclosure of KeyPoint's confidential information, trade secrets, and other secretive information that KeyPoint is obligated to strictly protect based on its contractual relationship with the United States Office of Personnel Management's ("OPM") National Background Investigations Bureau ("NBIB").

In support of its claims, KeyPoint alleges as follows:

THE PARTIES, JURISDICTION, AND VENUE

1. KeyPoint, by its attorneys, files this Complaint against Defendant.

2. KeyPoint provides specialized investigative and risk mitigation services to a variety of U.S. federal government agencies and organizations in the civilian, defense, and intelligence sectors.

3. KeyPoint is a corporation organized and incorporated under the laws of the State of Delaware. KeyPoint is headquartered in Loveland, Colorado.

4. Defendant, a Virginia resident and citizen, began his employment with KeyPoint in September 2011. His most recent position was "Regional Field Director" and he was based in Virginia. KeyPoint had promoted Defendant to the Regional Field Director position in October 2016. He resigned effective November 23, 2016.

5. Prior to his promotion to the position of Regional Field Director, Defendant worked in a variety of positions with KeyPoint, including Field Manager 3 OPM, Investigator, IACC Specialist, and Mentor.

6. This Court has jurisdiction over this action under 28 U.S.C. § 1332 because there is complete diversity of citizenship and KeyPoint's losses as a result of Defendant's unlawful actions, while impossible to calculate with precision, exceed $75,000.

7. Venue is proper in this judicial district under 28 U.S.C. § 1391(b)(1) and (2) because Defendant resides in this judicial district, and because a substantial part of the events or omissions giving rise to these claims occurred in this judicial district.

ADDITIONAL BACKGROUND AND SPECIFIC ALLEGATIONS

8. KeyPoint offers a variety of security clearance and other types of background investigations, inspection services, financial and other fraud investigation services, among other

things, primarily in support of various government agencies.

9. KeyPoint is obligated under its government contracts to provide specific investigative services to various federal agencies.

10. Currently, KeyPoint's largest client for background investigation services is the OPM's NBIB.

11. In general, OPM works to recruit and retain a workforce for the federal government. As a part of its mission, OPM/NBIB provides suitability and security background investigations in connection with prospective employees, employees, and contractors. KeyPoint assists with this critical process based on its contracts with OPM.

12. KeyPoint also contracts to provide background investigation services for the Department of Homeland Security ("DHS"), and other federal agencies.

13. KeyPoint is the largest provider of such services to the federal government, and these government contracts comprise the vast majority of KeyPoint's business. Without them, it is unlikely KeyPoint would survive. Therefore, KeyPoint goes to great lengths to remain in good standing with these agencies and to ensure it strictly complies with their requirements and procedures, and maintain the secrecy of their information.

14. KeyPoint's primary role in its investigations business is to provide fieldwork services via a network of cleared and trained employees and independent contractors. KeyPoint must ensure that its investigators and staff follow confidential security procedures dictated by KeyPoint's clients, including OPM and DHS.

15. KeyPoint has been entrusted with highly confidential information by OPM under federal contracts that strictly prohibit the external disclosure of the information. Any unauthorized disclosure of information entrusted by OPM to KeyPoint may threaten national

security interests.

16. KeyPoint's contract with OPM requires KeyPoint investigators to conduct investigations according to OPM's protocols and instructions. Pursuant to the publicly-available Solicitation provisions of OPM's contract with KeyPoint, OPM requires KeyPoint to strictly limit access to the Investigator's Handbook and "any training materials or other documents that contain information on OPM procedures" to personnel "who have been cleared by OPM to work on [the] Contract." OPM's contract also makes clear that any supplemental training materials developed by KeyPoint "are the property of OPM-FIS" and must be approved by OPM-FIS, accordingly. FIS is the Federal Investigation Services which was the name of NBIB before October 1, 2016.

17. In general, KeyPoint's investigations business consists of investigating individuals who seek either security clearance (or renewal of a clearance) for access to classified information or suitability (or continuing suitability) for particular positions either with the government or with a government contractor. The individual seeking a clearance is known as the "subject" of the investigation.

18. The nature of the clearance or the position determines the type of investigation services KeyPoint is contracted to perform. For example, an investigation might include a "subject interview," multiple "source interviews," law checks, education verification, records collections, employment verification, supervisor interviews, or neighborhood checks. Investigations conclude with a report of investigation which includes all information collected by the various investigators assigned to that case.

19. KeyPoint's clients award KeyPoint the work and KeyPoint then ensures that the work is performed pursuant to strict, highly confidential protocols provided by the clients.

20. OPM and KeyPoint's other clients require extensive training and credentialing before an individual may conduct investigations under its contract with KeyPoint. All staff working on these contracts undergo background investigations equivalent to those accessing Top Secret information. As an employee with KeyPoint for more than 5 years, and based on his work as an Investigator in addition to other position, Defendant was fully trained on the mandatory procedures for handling and processing OPM-related information and data.

21. OPM provides specific direction on how investigations must be conducted, who may conduct them, and who may have access to information regarding the investigation process. Many of these highly confidential investigation procedures are set out in the "OPM Handbook" along with associated policies.

22. The OPM Handbook is created by OPM. It lists, among other things, requirements from OPM about how an investigator must conduct investigations. The contract for services between OPM and KeyPoint requires that KeyPoint follow the OPM Handbook, and that KeyPoint strictly maintain the confidentiality of the information contained in the OPM Handbook. Similarly, KeyPoint has developed specific guidance on how to execute the directions contained in the OPM Handbook. Employees of KeyPoint are required to maintain the secrecy of the guides because they are based on and contain excerpts from the highly confidential OPM Handbook. Based on his employment and training with KeyPoint, Defendant was fully aware of the requirements to maintain the secrecy of the OPM Handbook and all KeyPoint guides relating to the OPM Handbook.

23. The OPM Handbook and any guides relating to the OPM Handbook may only be distributed to personnel specifically approved by OPM to work on the OPM contract, and such distribution is subject to audit by OPM. Any training materials or other documents that contain

information on OPM procedures must be controlled by KeyPoint in the same manner as the OPM Handbook, and must be maintained as strictly confidential.

24. As an example of the secrecy required for KeyPoint's work, KeyPoint's investigative personnel must compose reports of investigations pursuant to the guidelines of the OPM Handbook on an encrypted computer. It is imperative that all case information be *exclusively maintained* within a suite of systems designed, maintained, and controlled by OPM, unless otherwise permitted by OPM.

25. KeyPoint's personnel are prohibited from divulging or releasing program information developed or obtained in connection with the performance of the Contract to anyone other than as authorized by OPM personnel.

26. OPM ensures compliance with contract requirements through various means such as a review of administrative and managerial processes and investigative practices, on-site inspections, an assessment of investigative personnel while conducting work, and a quality review of completed fieldwork investigation.

27. In the course of his employment with KeyPoint, Defendant signed numerous acknowledgments regarding his confidentiality obligations to KeyPoint and regarding KeyPoint's duty of confidentiality to OPM and other clients. For example, on May 13, 2014, Defendant signed the "Investigator's Training Materials Acknowledgment/Collection Form" acknowledging receipt of an electronic copy of OPM's Investigator's Handbook, and agreeing that he may not copy or reproduce the Handbook in any way without the proper consent of the OPM. On October 25, 2011, Defendant signed an acknowledgment of the KeyPoint Code of Conduct which contains specific policies on the protection of KeyPoint and client information.

28. Defendant also entered into a "Classified Information and Non-Disclosure

Agreement" in consideration for being granted access to classified information in the course of his work with KeyPoint.

29. KeyPoint's business involves the development and use of trade secrets and highly confidential information, and KeyPoint focuses on developing long-term relationships with its clients and on developing trust and confidence in the services of KeyPoint.

30. KeyPoint has invested substantial time, expense, and resources in its business to build its reputation, image and relationships with its clients, and KeyPoint has established a valuable and substantial reputation, trade, and patronage as an industry leader and expert. KeyPoint has also invested significant time, expense and resources to create and maintain its client relationships.

31. KeyPoint maintains confidential information and trade secrets that are valuable, confidential, and proprietary to KeyPoint, and also maintains confidential information that must be maintained as secret for its clients. KeyPoint has expended substantial effort and incurred substantial expense in developing and maintaining such confidential information and trade secrets, and in maintaining the secrecy of its clients' information, and KeyPoint has a legitimate business interest in keeping such information confidential, and not allowing the information to be disclosed to, or used by any improper means.

32. To protect the legitimate business interests identified above, and to ensure compliance with its obligations to the OPM and other clients, KeyPoint also prohibits its employees from disclosing confidential information and trade secrets, and KeyPoint has taken and continues to take additional measures to protect its confidential information and trade secrets, and the secrecy of its clients' information.

33. During his employment with KeyPoint, Defendant gained detailed and intimate

knowledge of KeyPoint's confidential information and trade secrets, and of the secret and classified information of its clients. The information is unique to KeyPoint and its clients and was disclosed to Defendant solely due to his employment relationship with KeyPoint and in reliance on his commitment to keep that information strictly confidential.

34. Defendant's resignation from KeyPoint was effective November 23, 2016. Defendant is now employed by a competitor of KeyPoint.

35. Another former employee of KeyPoint, Daniel Pierron, resigned from KeyPoint on January 3, 2017, and he joined the same company that now employs Defendant McGinn. After Daniel Pierron resigned, KeyPoint learned of information that led KeyPoint to conduct an analysis of Mr. Pierron's KeyPoint computer and e-mail communication. KeyPoint's analysis revealed that in direct violation of his obligations to KeyPoint, and in direct violation of the mandatory procedures of KeyPoint and its clients, Mr. Pierron had sent numerous highly confidential records to his personal email address immediately prior to his resignation from KeyPoint. Based on KeyPoint's analysis, KeyPoint learned that Mr. Pierron had sent to his personal e-mail address and maintained copies of KeyPoint's confidential and proprietary information, including but not limited to documents and information relating to KeyPoint's recruiting strategies, secret materials used by KeyPoint regarding OPM's Handbook, internal analysis conducted by KeyPoint regarding the use of certain technology to communicate with Investigators, training materials, and other proprietary internal analysis conducted by KeyPoint.

36. Based on KeyPoint's analysis of Daniel Pierron's activity, on April 3, 2017, KeyPoint filed a Complaint against Daniel Pierron in the United States District Court, Southern District of Ohio. KeyPoint subsequently obtained a Temporary Restraining Order and a Preliminary Injunction against Daniel Pierron.

37. As a part of the pending litigation against Daniel Pierron, on Monday, July 31, 2017, the attorneys for KeyPoint took the deposition of Daniel Pierron. During that deposition KeyPoint learned for the first time that Daniel Pierron had, without authorization, provided *to Defendant McGinn* the confidential information, trade secrets, and OPM-related information and data that Daniel Pierron had removed from KeyPoint. (Deposition transcript of Daniel Pierron, July 31, 2017, pages 59-61). Daniel Pierron testified that during the course of his employment with his new employer, and while working with Defendant McGinn at his new employer, he had provided Defendant McGinn with a "thumb-drive" that contained the highly confidential information that Mr. Pierron had removed from KeyPoint. (Deposition transcript of Daniel Pierron, July 31, 2017, pages 59-60). Daniel Pierron also testified during his deposition that he personally observed Defendant McGinn attach the thumb-drive to his employer's computer and that Defendant McGinn downloaded the KeyPoint and OPM-related information to the new employer's computer. *Id.* OPM prohibits the transfer of information between vendors by any method even when the individual will continue to work on the program for a different contractor in order to ensure their control over the information.

38. Daniel Pierron further testified during his deposition that he subsequently lost the thumb-drive that contained the KeyPoint and OPM-related information he had improperly removed from KeyPoint. After Mr. Pierron lost the thumb-drive, he met with Defendant McGinn at their new employer's offices in Virginia and made another full copy of the confidential KeyPoint and OPM-related information that Defendant McGinn had copied from Daniel Pierron. As Daniel Pierron testified, the confidential KeyPoint and OPM-related information had remained on Defendant McGinn's work computer, and Defendant McGinn was with Daniel Pierron when the copy of the confidential information was once again transferred to a thumb-

drive from Defendant McGinn's work computer. (Deposition transcript of Daniel Pierron, July 31, 2017, pages 61-62).

COUNT I
MISAPPROPRIATION OF TRADE SECRETS

39. KeyPoint incorporates and re-alleges the foregoing paragraphs as though fully set forth herein.

40. KeyPoint has maintained and developed highly valuable trade secrets and other confidential information which are safeguarded as confidential and protected from direct or indirect disclosure to outside persons and entities. KeyPoint also has an obligation to maintain the secrecy of information entrusted to it by clients.

41. KeyPoint has taken reasonable precautions to preserve the secrecy of its trade secrets and confidential information.

42. KeyPoint's information has independent economic value from not being generally known to, and not being readily ascertainable by proper means.

43. KeyPoint's trade secrets and other confidential information are extremely valuable and critical to the operation of KeyPoint's business and to its clients, including OPM.

44. Virginia law recognizes the protection of a company's trade secrets against actual or threatened misappropriation, and the Virginia Uniform Trade Secrets Act provides that actual or threatened misappropriation of trade secrets may be enjoined, and that damages may be awarded.

45. During his employment with KeyPoint, Defendant was provided and had access to KeyPoint's trade secret information and other confidential and proprietary information including information relating to OPM that KeyPoint is required to maintain as confidential and

upon information and belief Defendant has retained such information.

46. Upon information and belief, Defendant has used, revealed, and otherwise disclosed (or will inevitably disclose) KeyPoint's valuable trade secrets and other confidential and proprietary information, including information of its clients that it is obligated to maintain as secret.

47. Defendant's conduct constitutes the actual or threatened misappropriation, misuse, and/or inevitable reliance upon KeyPoint's confidential, proprietary, and trade secret information in violation of the Virginia Uniform Trade Secrets Act.

48. Defendant's actions, including the use or disclosure of KeyPoint's trade secrets and confidential information, violates the Virginia Uniform Trade Secrets Act, and has caused damage to KeyPoint.

49. Defendant's misappropriation and/or threatened misappropriation of KeyPoint's trade secrets and confidential information is willful and malicious.

50. As a result of Defendant's misappropriation and/or threatened misappropriation of its trade secrets and confidential information, KeyPoint has suffered and will continue to suffer damages, as well as irreparable harm. KeyPoint has been damaged by the misappropriation of its trade secrets and confidential information by, among things: the loss of confidential and proprietary information; injury to its reputation; actual and potential loss of sales, revenues, and profits; and attorneys' fees and costs.

51. As a result of Defendant's misappropriation and/or threatened misappropriation of KeyPoint's trade secrets, KeyPoint has suffered and will suffer substantial harm and damages.

52. Unless Defendant is enjoined from disclosing and/or utilizing KeyPoint's confidential information, Plaintiff will continue to be immediately and irreparably harmed.

53. KeyPoint has no adequate remedy at law.

COUNT II
CONVERSION

54. KeyPoint incorporates the foregoing paragraphs as though fully set forth herein.

55. Defendant has misappropriated and converted to his own use the proprietary business records and documents of KeyPoint.

56. At all relevant times, KeyPoint owned and was entitled to exclusive use of its efforts and work, as well as to existing files, analysis, lists, and processes as contained within its computer systems and records.

57. In doing the acts described above, Defendant has misappropriated the property and assets of KeyPoint by diverting and converting said proprietary business records and documents for his own use despite Defendant's obligation to return the property and assets to KeyPoint.

58. As a direct, proximate, and foreseeable result of Defendant's conduct, KeyPoint has suffered and continues to suffer substantial losses and damages in an amount to be proven at trial.

59. The aforementioned acts of Defendant were willful and oppressive, fraudulent or malicious entitling KeyPoint to recover punitive and exemplary damages from Defendant in an amount to be determined at trial.

60. Defendant has threatened to, and unless restrained, will continue to use the misappropriated property and assets of KeyPoint in the form of proprietary business records and documents.

61. KeyPoint has suffered and will suffer substantial harm for which there is no adequate remedy at law.

INJUNCTIVE RELIEF and OTHER RELIEF

62. Unless Defendant is enjoined from the aforementioned conduct, KeyPoint will be irreparably harmed by the misappropriation of its confidential information and trade secrets, loss of goodwill, loss of reputation, and present and future economic loss.

63. KeyPoint has already suffered and will continue to suffer irreparable injury and harm to its business, and monetary damages are an inadequate redress for such continuing injury.

64. KeyPoint has no adequate remedy at law and is entitled to injunctive relief.

WHEREFORE, KeyPoint demands judgment as follows:

A. A temporary restraining order, and a preliminary and permanent injunction enjoining and restraining Defendant, including an order for Defendant and any third-party to whom Defendant has disclosed or shared Plaintiff's or its clients' information to:

1. Immediately identify for KeyPoint and its counsel all KeyPoint and client information and data (including all confidential information and trade secrets of KeyPoint and its clients) McGinn maintained, transferred, or transmitted by any means without authorization during or after his employment with KeyPoint;

2. Immediately, and pursuant to a protocol agreed to by KeyPoint, return to KeyPoint all KeyPoint and client information and data (including all memoranda, notes, lists, records, e-mails, computer files, and other documents and information, and all copies and versions thereof);

3. Preserve and protect in their present state from destruction, modification, or alteration all information, data, and documents relating to KeyPoint and its clients in any form (including any information and data stored on any computers or electronic devices over which McGinn has possession, custody, or control), including, as well, the preservation and protection of all emails in any account over which he has access, and any information, documents, or data that may be relevant or discoverable in this case; and

4. Immediately produce, pursuant to a protocol agreed to by KeyPoint, all personal, home, and/or professional computers, servers, electronic storage devices, mobile devices, and e-mail accounts on which there has been any of KeyPoint's or its clients' information or data, or which McGinn has used to access, view, or disseminate any of KeyPoint's or its clients'

information or data, and that are in his possession, custody, or control, to an authorized third-party computer forensics expert as designated by KeyPoint to review those computers, electronic storage devices, and e-mail accounts.

KeyPoint also seeks an order that McGinn and any third-party to whom Defendant has disclosed or shared Plaintiff's or its clients' information shall not use or disclose to any third party, including his current employer, any material (including all documents and data) relating to KeyPoint and its clients, including KeyPoint's or its clients' confidential material and trade secrets.

B. Compensatory damages in an amount exceeding $75,000.00;

C. Punitive and exemplary damages in an amount exceeding $75,000.00;

D. An award of costs incurred in the prosecution of this action, including reasonable attorneys' fees and costs;

E. Interest; and

F. Such other and further relief, legal and equitable, that this Court deems just and proper.

JURY DEMAND

Plaintiff demands a jury of eight on all issues triable by a jury.

Dated: August 8, 2017.

Respectfully submitted,

/s/ Joon Hwang
Joon Hwang (VSB # 82248)
Littler Mendelson, P.C.
1650 Tysons Blvd., Suite 700
McLean, Virginia 22102
(703) 286-3136 (Telephone)
(703) 373-2628 (Facsimile)
jhwang@littler.com

Attorneys for Plaintiff KeyPoint Government Solutions, Inc.

Firmwide:149325601.1 063273.1000

VERIFICATION

STATE OF Colorado :
: **SS**
COUNTY OF Larimer :

Angela Deabler deposes and states that she is the Senior Vice President and Program Director, OPM, at KeyPoint Government Solutions, Inc.; that she has read the foregoing Verified Complaint; that this verification is based upon the information available to KeyPoint Government Solutions, Inc. and that to the best of her knowledge, information, and belief, the allegations in the foregoing Verified Complaint are true.

Angela Deabler

Sworn to and subscribed in my presence this 7th day of August, 2017

MARISSA BLACKWOOD
NOTARY PUBLIC - STATE OF COLORADO
Notary Identification #20164029659
My Commission Expires 8/4/2020

Notary Public